Cartilha de Segurança para Internet

Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção

Versão 3.0
Setembro de 2005
http://cartilha.cert.br/

cgi.br

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção

Esta parte da Cartilha aborda diversos riscos envolvidos no uso da Internet e seus métodos de prevenção. São discutidos os programas que possibilitam aumentar a segurança de um computador, como antivírus e *firewalls*, e apresentados riscos e medidas preventivas no uso de programas leitores de *e-mails*, *browsers*, programas de troca de mensagens, de distribuição de arquivos e recursos de compartilhamento de arquivos. Também é discutida a importância da realização de cópias de segurança.

Versão 3.0 – Setembro de 2005
http://cartilha.cert.br/

Sumário

1 Programas Leitores de *E-mails*

1.1 Quais são os riscos associados ao uso de um programa leitor de *e-mails*?

Grande parte dos problemas de segurança envolvendo *e-mails* estão relacionados aos conteúdos das mensagens, que normalmente abusam das técnicas de engenharia social (vide partes I: Conceitos de Segurança e IV: Fraudes na Internet) ou de características de determinados programas leitores de *e-mails*, que permitem abrir arquivos ou executar programas anexados às mensagens automaticamente.

1.2 É possível configurar um programa leitor de *e-mails* de forma mais segura?

Sim. Algumas dicas de configuração para melhorar a segurança do seu programa leitor de *e-mails* são:

1. desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
2. desligar as opções de execução de *JavaScript* e de programas *Java* (vide seção 2.2);
3. desligar, se possível, o modo de visualização de *e-mails* no formato HTML (mais detalhes nas partes IV: Fraudes na Internet e VI: *Spam*).

Estas configurações podem evitar que o seu programa leitor de *e-mails* propague automaticamente vírus e cavalos de tróia, entre outros. Existem programas leitores de *e-mails* que não implementam tais funções e, portanto, não possuem estas opções.

É importante ressaltar que se o usuário seguir as recomendações dos itens 1 e 2, mas ainda assim abrir os arquivos ou executar manualmente os programas que vêm anexados aos *e-mails*, poderá ter algum problema que resulte na violação da segurança do seu computador.

1.3 Que medidas preventivas devo adotar no uso dos programas leitores de *e-mails*?

Algumas medidas preventivas que minimizam os problemas trazidos com os *e-mails* são:

- manter sempre a versão mais atualizada do seu programa leitor de *e-mails*;
- não clicar em *links* que, por ventura, possam aparecer no conteúdo do *e-mail*. Se você realmente quiser acessar a página do *link*, digite o endereço diretamente no seu *browser*, seguindo as orientações da seção 2.7;
- evitar abrir arquivos ou executar programas anexados aos *e-mails*, sem antes verificá-los com um antivírus;

- desconfiar sempre dos arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado[1] e o arquivo anexo pode ser, por exemplo, um vírus ou um cavalo de tróia;
- fazer o *download* de programas diretamente do *site* do fabricante;
- evitar utilizar o seu programa leitor de *e-mails* como um *browser*, desligando o modo de visualização de *e-mails* no formato HTML.

Atualmente, usuários da Internet têm sido bombardeados com *e-mails* indesejáveis e, principalmente, com mensagens fraudulentas cuja finalidade é a obtenção de vantagens financeiras. Alguns exemplos são:

- mensagens oferecendo grandes quantias em dinheiro, mediante uma transferência eletrônica de fundos;
- mensagens com ofertas de produtos com preços muito abaixo dos preços praticados pelo mercado;
- mensagens que procuram induzir o usuário a acessar uma determinada página na Internet ou a instalar um programa, abrir um álbum de fotos, ver cartões virtuais, etc, mas cujo verdadeiro intuito é fazer com que o usuário forneça dados pessoais e sensíveis, como contas bancárias, senhas e números de cartões de crédito.

Mais detalhes sobre estes tipos de *e-mail*, bem como formas de prevenção, podem ser vistos na parte IV: Fraudes na Internet.

2 *Browsers*

2.1 Quais são os riscos associados ao uso de um *browser*?

Existem diversos riscos envolvidos na utilização de um *browser*. Dentre eles, podem-se citar:

- execução de *JavaScript* ou de programas *Java* hostis;
- execução de programas ou controles *ActiveX* hostis;
- obtenção e execução de programas hostis em *sites* não confiáveis ou falsos;
- acesso a *sites* falsos, se fazendo passar por instituições bancárias ou de comércio eletrônico;
- realização de transações comerciais ou bancárias via *Web*, sem qualquer mecanismo de segurança.

Nos dois primeiros casos o *browser* executa os programas automaticamente, ou seja, sem a interferência do usuário.

[1] Existem vírus e outros tipos de *software* malicioso que utilizam o *e-mail* como meio para sua propagação e quase sempre forjam o endereço do remetente.

2.2 Quais são os riscos associados à execução de *JavaScripts* e de programas *Java*?

Normalmente os *browsers* contêm módulos específicos para processar programas *Java*. Apesar destes módulos fornecerem mecanismos de segurança, podem conter falhas de implementação e, neste caso, permitir que um programa *Java* hostil cause alguma violação de segurança em um computador.

JavaScripts, entre outros *scripts Web* disponíveis, são muito utilizados atualmente para incorporar maior funcionalidade e melhorar a aparência de páginas *Web*. Apesar de nem sempre apresentarem riscos, vêm sendo utilizados por atacantes para causar violações de segurança em computadores. Um tipo de ataque envolvendo *JavaScript* consiste em redirecionar usuários de um *site* legítimo para um *site* falso, para que o usuário instale programas maliciosos ou forneça informações pessoais.

2.3 Quais são os riscos associados à execução de programas *ActiveX*?

Antes de receber um programa *ActiveX*, o seu *browser* verifica sua procedência através de um esquema de certificados digitais (vide partes I: Conceitos de Segurança e IV: Fraudes na Internet). Se você optar por aceitar o certificado, o programa é executado em seu computador.

Ao serem executados, os programas *ActiveX* podem fazer de tudo, desde enviar um arquivo qualquer pela Internet, até instalar programas (que podem ter fins maliciosos) em seu computador.

2.4 Quais são os riscos associados ao uso de *cookies*?

Muitos *sites* utilizam *cookies* para obter informações, como por exemplo, as preferências de um usuário. Estas informações, muitas vezes, são compartilhadas entre diversas entidades na Internet e podem afetar a privacidade do usuário.

Maiores detalhes sobre os riscos envolvidos no uso de *cookies*, bem como formas de se ter maior controle sobre eles, podem ser vistos na parte III: Privacidade.

2.5 Quais são os riscos associados às *pop-up windows*?

Pop-up windows são janelas que aparecem automaticamente e sem permissão, sobrepondo a janela do *browser*, após o usuário acessar um *site*. Este recurso tem sido amplamente utilizado para apresentar mensagens com propaganda para usuários da Internet e, por este motivo, tem sido também classificado como *pop-up spam*.

Em muitos casos, as mensagens contidas nas *pop-up windows* apresentam *links*, que podem redirecionar o usuário para uma página fraudulenta ou induzí-lo a instalar algum *software* malicioso para, por exemplo, furtar senhas bancárias ou números de cartões de crédito. Exemplos do uso malicioso de *pop-up windows* podem ser vistos na parte IV: Fraudes na Internet.

2.6 Quais são os cuidados necessários para realizar transações via *Web*?

Normalmente as transações, sejam comerciais ou bancárias, envolvem informações sensíveis, como senhas ou números de cartões de crédito.

Portanto, é muito importante que você, ao realizar transações via *Web*, certifique-se da procedência dos *sites* e se estes *sites* são realmente das instituições que dizem ser. Também é fundamental que eles forneçam mecanismos de segurança para evitar que alguém conectado à Internet possa obter informações sensíveis de suas transações, no momento em que estiverem sendo realizadas.

Maiores detalhes sobre estes cuidados, bem como formas de prevenção na realização de transações via *Web* podem ser vistos na parte IV: Fraudes na Internet.

2.7 Que medidas preventivas devo adotar no uso de *browsers*?

Algumas medidas preventivas para o uso de *browsers* são:

- manter o seu *browser* sempre atualizado;
- desativar a execução de programas *Java* na configuração de seu *browser*[2]. Se for absolutamente necessário o *Java* estar ativado para que as páginas de um *site* possam ser vistas, basta ativá-lo antes de entrar no *site* e, então, desativá-lo ao sair;
- desativar a execução de *JavaScripts* antes de entrar em uma página desconhecida e, então, ativá-la ao sair. Caso você opte por desativar a execução de *JavaScripts* na configuração de seu *browser*, é provável que muitas páginas *Web* não possam ser visualizadas;
- permitir que programas *ActiveX* sejam executados em seu computador **apenas** quando vierem de *sites* conhecidos e confiáveis;
- manter maior controle sobre o uso de *cookies*, caso você queira ter maior privacidade ao navegar na Internet (vide parte III: Privacidade);
- bloquear *pop-up windows* e permití-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- certificar-se da procedência do *site* e da utilização de conexões seguras ao realizar transações via *Web* (vide parte IV: Fraudes na Internet);
- somente acessar *sites* de instituições financeiras e de comércio eletrônico digitando o endereço diretamente no seu *browser*, nunca clicando em um *link* existente em uma página ou em um *e-mail*. Assim, você pode evitar ser redirecionado para uma página fraudulenta ou ser induzido a instalar algum *software* malicioso, que tem como objetivo furtar seus dados pessoais (incluindo senhas e números de cartões de crédito).

[2] Os programas *Java* não são utilizados na maioria das páginas *Web* e, quando utilizados, a desativação de sua execução não costuma comprometer a visualização da página.

2.8 Que características devo considerar na escolha de um *browser*?

Existem características muito importantes que você deve considerar no momento de escolher um *browser*. Algumas destas características são:

- histórico de vulnerabilidades associadas ao *browser* e o tempo decorrido entre a descoberta da vulnerabilidade e o lançamento da correção;
- **não** instalação/execução automática de programas;
- facilidade para identificar se o *site* usa conexão segura e para visualizar dados do certificado digital;
- disponibilidade de mecanismos para desabilitar a execução de programas *Java*, *JavaScript*, *ActiveX*, entre outros;
- disponibilidade de mecanismos que permitam bloquear (incluindo bloqueio seletivo) *cookies* e *pop-up windows*.

3 Antivírus

Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador. Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia e outros tipos de código malicioso[3], barrar programas hostis e verificar *e-mails*.

3.1 Que funcionalidades um bom antivírus deve possuir?

Um bom antivírus deve:

- identificar e eliminar a maior quantidade possível de vírus e outros tipos de *malware*;
- analisar os arquivos que estão sendo obtidos pela Internet;
- verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e *pen drives*, de forma transparente ao usuário;
- procurar vírus, cavalos de tróia e outros tipos de *malware* em arquivos anexados aos *e-mails*;
- criar, sempre que possível, uma mídia de verificação (disquete ou CD de *boot*) que possa ser utilizado caso um vírus desative o antivírus que está instalado no computador;
- atualizar as assinaturas de vírus e *malwares* conhecidos, pela rede, de preferência diariamente.

Alguns antivírus, além das funcionalidades acima, permitem verificar *e-mails* enviados, podendo detectar e barrar a propagação por *e-mail* de vírus, *worms*, e outros tipos de *malware*.

[3] A definição de código malicioso (*malware*) pode ser encontrada na parte I: Conceitos de Segurança.

3.2 Como faço bom uso do meu antivírus?

As dicas para o bom uso do antivírus são simples:

- mantenha o antivírus e suas assinaturas sempre atualizados;
- configure-o para verificar automaticamente arquivos anexados aos *e-mails* e arquivos obtidos pela Internet;
- configure-o para verificar automaticamente mídias removíveis (CDs, DVDs, *pen drives*, disquetes, discos para Zip, etc);
- configure-o para verificar todo e qualquer formato de arquivo (qualquer tipo de extensão de arquivo);
- se for possível, crie o disquete de verificação e utilize-o esporadicamente, ou quando seu computador estiver apresentando um comportamento anormal (mais lento, gravando ou lendo o disco rígido fora de hora, etc);

Algumas versões de antivírus são gratuitas para uso pessoal e podem ser obtidas pela Internet. Mas antes de obter um antivírus pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável.

3.3 O que um antivírus não pode fazer?

Um antivírus não é capaz de impedir que um atacante tente explorar alguma vulnerabilidade (vide seção 5) existente em um computador. Também não é capaz de evitar o acesso não autorizado a um *backdoor*[4] instalado em um computador.

Existem também outros mecanismos de defesa, conhecidos como *firewalls*, que podem prevenir contra tais ameaças (vide seção 4);

4 *Firewalls*

Os *firewalls* são dispositivos constituídos pela combinação de *software* e *hardware*, utilizados para dividir e controlar o acesso entre redes de computadores.

Um tipo específico é o ***firewall* pessoal**, que é um *software* ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet.

4.1 Como o *firewall* pessoal funciona?

Se alguém ou algum programa suspeito tentar se conectar ao seu computador, um *firewall* bem configurado entra em ação para bloquear tentativas de invasão, podendo barrar também o acesso a *backdoors*, mesmo se já estiverem instalados em seu computador.

[4] Detalhes sobre *backdoors* podem ser vistos na parte VIII: Códigos Maliciosos (*Malware*).

Alguns programas de *firewall* permitem analisar continuamente o conteúdo das conexões, filtrando vírus de *e-mail*, cavalos de tróia e outros tipos de *malware*, antes mesmo que os antivírus entrem em ação.

Também existem pacotes de *firewall* que funcionam em conjunto com os antivírus, provendo um maior nível de segurança para os computadores onde são utilizados.

4.2 Por que devo instalar um *firewall* pessoal em meu computador?

É comum observar relatos de usuários que acreditam ter computadores seguros por utilizarem apenas programas antivírus. O fato é que a segurança de um computador não pode basear-se apenas em **um** mecanismo de defesa.

Um antivírus não é capaz de impedir o acesso a um *backdoor* instalado em um computador. Já um *firewall* bem configurado pode bloquear o acesso a ele.

Além disso, um *firewall* poderá bloquear as tentativas de invasão ao seu computador e possibilitar a identificação das origens destas tentativas.

Alguns fabricantes de *firewalls* oferecem versões gratuitas de seus produtos para uso pessoal. Mas antes de obter um *firewall*, verifique sua procedência e certifique-se que o fabricante é confiável.

4.3 Como posso saber se estão tentando invadir meu computador?

Normalmente os *firewalls* criam arquivos em seu computador, denominados arquivos de registro de eventos (*logs*). Nestes arquivos são armazenadas as tentativas de acesso não autorizado ao seu computador, para serviços que podem ou não estar habilitados.

A parte VII: Incidentes de Segurança e Uso Abusivo da Rede apresenta um guia para que você não só identifique tais tentativas, mas também reporte-as para os responsáveis pela rede ou computador de onde a tentativa de invasão se originou.

5 Vulnerabilidades

5.1 Como posso saber se os *softwares* instalados em meu computador possuem alguma vulnerabilidade?

Existem *sites* na Internet que mantêm listas atualizadas de vulnerabilidades em *softwares* e sistemas operacionais. Alguns destes *sites* são `http://www.cert.org/`, `http://cve.mitre.org/` e `http://www.us-cert.gov/cas/alerts/`.

Além disso, fabricantes também costumam manter páginas na Internet com considerações a respeito de possíveis vulnerabilidades em seus *softwares*.

Portanto, a idéia é estar sempre atento aos *sites* especializados em acompanhar vulnerabilidades, aos *sites* dos fabricantes, às revistas especializadas e aos cadernos de informática dos jornais, para verificar a existência de vulnerabilidades no sistema operacional e nos *softwares* instalados em seu computador.

5.2 Como posso corrigir as vulnerabilidades dos *softwares* em meu computador?

A melhor forma de evitar que o sistema operacional e os *softwares* instalados em um computador possuam vulnerabilidades é mantê-los **sempre atualizados**.

Entretanto, fabricantes em muitos casos não disponibilizam novas versões de seus *softwares* quando é descoberta alguma vulnerabilidade, mas sim correções específicas (*patches*). Estes *patches*, em alguns casos também chamados de *hot fixes* ou *service packs*, têm por finalidade corrigir os problemas de segurança referentes às vulnerabilidades descobertas.

Portanto, é **extremamente importante** que você, além de manter o sistema operacional e os *softwares* sempre atualizados, instale os *patches* sempre que forem disponibilizados.

6 Programas de Troca de Mensagens

6.1 Quais são os riscos associados ao uso de salas de bate-papo e de programas como o ICQ ou IRC?

Os maiores riscos associados ao uso destes programas estão no conteúdo dos próprios diálogos. Alguém pode utilizar técnicas de engenharia social (vide partes I: Conceitos de Segurança e IV: Fraudes na Internet) para obter informações (muitas vezes sensíveis) dos usuários destes programas.

Você pode ser persuadido a fornecer em uma conversa "amigável" seu *e-mail*, telefone, endereço, senhas (como a de acesso ao seu provedor), número do seu cartão de crédito, etc. As conseqüências podem ser desde o recebimento de mensagens com conteúdo falso/alarmante ou mensagens não solicitadas contendo propagandas, até a utilização da conta no seu provedor para realizar atividades ilícitas ou a utilização de seu número de cartão de crédito para fazer compras em seu nome (vide parte IV: Fraudes na Internet).

Além disso, estes programas podem fornecer o seu endereço na Internet (endereço IP[5]). Um atacante pode usar esta informação para, por exemplo, tentar explorar uma possível vulnerabilidade em seu computador.

6.2 Existem problemas de segurança específicos nos programas de troca instantânea de mensagens?

Programas, tais como o ICQ, AOL Instant Messenger, Yahoo! Messenger e MSN Messenger, por se comunicarem constantemente com um servidor (senão não teriam como saber quem está no ar), ficam mais expostos e sujeitos a ataques, caso possuam alguma vulnerabilidade.

[5] O significado de endereço IP pode ser encontrado no Glossário.

6.3 Que medidas preventivas devo adotar no uso de programas de troca de mensagens?

Algumas medidas preventivas para o uso de programas de troca de mensagens são:

- manter seu programa de troca de mensagens sempre atualizado, para evitar que possua alguma vulnerabilidade (vide seção 5);
- não aceitar arquivos de pessoas desconhecidas, principalmente programas de computadores;
- utilizar um bom antivírus, sempre atualizado, para verificar todo e qualquer arquivo ou *software* obtido através do programa de troca de mensagens, mesmo que venha de pessoas conhecidas;
- evitar fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;
- configurar o programa para ocultar o seu endereço IP.

7 Programas de Distribuição de Arquivos

7.1 Quais são os riscos associados ao uso de programas de distribuição de arquivos?

Existem diversos riscos envolvidos na utilização de programas de distribuição de arquivos, tais como o Kazaa, Morpheus, Edonkey, Gnutella e BitTorrent. Dentre estes riscos, podem-se citar:

Acesso não autorizado: o programa de distribuição de arquivos pode permitir o acesso não autorizado ao seu computador, caso esteja mal configurado ou possua alguma vulnerabilidade;

***Softwares* ou arquivos maliciosos:** os *softwares* ou arquivos distribuídos podem ter finalidades maliciosas. Podem, por exemplo, conter vírus, ser um *bot* ou cavalo de tróia, ou instalar *backdoors* em um computador;

Violação de direitos autorais (*Copyright*): a distribuição não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação desta lei.

7.2 Que medidas preventivas devo adotar no uso de programas de distribuição de arquivos?

Algumas medidas preventivas para o uso de programas de distribuição de arquivos são:

- manter seu programa de distribuição de arquivos sempre atualizado e bem configurado;

- ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo obtido, pois eles podem conter vírus, cavalos de tróia, entre outros tipos de *malware*;
- certificar-se que os arquivos obtidos ou distribuídos são **livres**, ou seja, não violam as leis de direitos autorais.

8 Compartilhamento de Recursos do Windows

8.1 Quais são os riscos associados ao uso do compartilhamento de recursos?

Um recurso compartilhado aparece no Explorer do Windows como uma "mãozinha" segurando a parte de baixo do ícone (pasta, impressora ou disco), como mostra a figura 1.

Figura 1: Exemplos de ícones para recursos compartilhados.

Alguns dos riscos envolvidos na utilização de recursos compartilhados por terceiros são:

- abrir arquivos ou executar programas que contenham vírus;
- executar programas que sejam cavalos de tróia ou outros tipos de *malware*.

Já alguns dos riscos envolvidos em compartilhar recursos do seu computador são:

- permitir o acesso não autorizado a recursos ou informações sensíveis;
- permitir que um atacante possa utilizar tais recursos, sem quaisquer restrições, para fins maliciosos. Isto pode ocorrer se não forem definidas senhas para os compartilhamentos.

8.2 Que medidas preventivas devo adotar no uso do compartilhamento de recursos?

Algumas medidas preventivas para o uso do compartilhamento de recursos do Windows são:

- ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo ou programa compartilhado, pois eles podem conter vírus ou cavalos de tróia, entre outros tipos de *malware*;
- estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador. Procure elaborar senhas fáceis de lembrar e difíceis de serem descobertas (vide parte I: Conceitos de Segurança).

É importante ressaltar que você deve sempre utilizar senhas para os recursos que deseje compartilhar, principalmente os que estão habilitados para leitura e escrita. E, quando possível, não compartilhe recursos ou não deixe-os compartilhados por muito tempo.

9 Realização de Cópias de Segurança (*Backups*)

9.1 Qual é a importância de fazer cópias de segurança?

Cópias de segurança dos dados armazenados em um computador são importantes, não só para se recuperar de eventuais falhas, mas também das conseqüências de uma possível infecção por vírus, ou de uma invasão.

9.2 Quais são as formas de realizar cópias de segurança?

Cópias de segurança podem ser simples como o armazenamento de arquivos em CDs ou DVDs, ou mais complexas como o espelhamento de um disco rígido inteiro em um outro disco de um computador.

Atualmente, uma unidade gravadora de CDs/DVDs e um *software* que possibilite copiar dados para um CD/DVD são suficientes para que a maior parte dos usuários de computadores realizem suas cópias de segurança.

Também existem equipamentos e *softwares* mais sofisticados e específicos que, dentre outras atividades, automatizam todo o processo de realização de cópias de segurança, praticamente sem intervenção do usuário. A utilização de tais equipamentos e *softwares* envolve custos mais elevados e depende de necessidades particulares de cada usuário.

9.3 Com que freqüência devo fazer cópias de segurança?

A freqüência com que é realizada uma cópia de segurança e a quantidade de dados armazenados neste processo depende da periodicidade com que o usuário cria ou modifica arquivos. Cada usuário deve criar sua própria política para a realização de cópias de segurança.

9.4 Que cuidados devo ter com as cópias de segurança?

Os cuidados com cópias de segurança dependem das necessidades do usuário. O usuário deve procurar responder algumas perguntas antes de adotar um ou mais cuidados com suas cópias de segurança:

- Que informações realmente importantes precisam estar armazenadas em minhas cópias de segurança?
- Quais seriam as conseqüências/prejuízos, caso minhas cópias de segurança fossem destruídas ou danificadas?
- O que aconteceria se minhas cópias de segurança fossem furtadas?

Baseado nas respostas para as perguntas anteriores, um usuário deve atribuir maior ou menor importância a cada um dos cuidados discutidos abaixo.

Escolha dos dados. Cópias de segurança devem conter apenas arquivos confiáveis do usuário, ou seja, que não contenham vírus e nem sejam algum outro tipo de *malware*. Arquivos do sistema operacional e que façam parte da instalação dos *softwares* de um computador não devem fazer parte das cópias de segurança. Eles podem ter sido modificados ou substituídos por versões maliciosas, que quando restauradas podem trazer uma série de problemas de segurança para um computador. O sistema operacional e os *softwares* de um computador podem ser reinstalados de mídias confiáveis, fornecidas por fabricantes confiáveis.

Mídia utilizada. A escolha da mídia para a realização da cópia de segurança é extremamente importante e depende da importância e da vida útil que a cópia deve ter. A utilização de alguns disquetes para armazenar um pequeno volume de dados que estão sendo modificados constantemente é perfeitamente viável. Mas um grande volume de dados, de maior importância, que deve perdurar por longos períodos, deve ser armazenado em mídias mais confiáveis, como por exemplo os CDs ou DVDs.

Local de armazenamento. Cópias de segurança devem ser guardadas em um local condicionado (longe de muito frio ou muito calor) e restrito, de modo que apenas pessoas autorizadas tenham acesso a este local (segurança física).

Cópia em outro local. Cópias de segurança podem ser guardadas em locais diferentes. Um exemplo seria manter uma cópia em casa e outra no escritório. Também existem empresas especializadas em manter áreas de armazenamento com cópias de segurança de seus clientes. Nestes casos é muito importante considerar a segurança física de suas cópias, como discutido no item anterior.

Criptografia dos dados. Os dados armazenados em uma cópia de segurança podem conter informações sigilosas. Neste caso, os dados que contenham informações sigilosas devem ser armazenados em algum formato criptografado.

9.5 Que cuidados devo ter ao enviar um computador para a manutenção?

É muito importante fazer cópias de segurança dos dados de um computador antes que ele apresente algum problema e seja necessário enviá-lo para manutenção ou assistência técnica.

Em muitos casos, o computador pode apresentar algum problema que impossibilite a realização de uma cópia de segurança dos dados antes de enviá-lo para a manutenção. Portanto, é muito importante que o usuário tenha disponível cópias de segurança recentes de seus dados. Não se pode descartar a possibilidade de, ao receber seu computador, ter a infeliz surpresa que todos os seus dados foram apagados durante o processo de manutenção.

Tenha sempre em mente que procurar uma assistência técnica de confiança é fundamental, principalmente se existirem dados sensíveis armazenados em seu computador, como declaração de Imposto de Renda, documentos e outras informações sigilosas, certificados digitais, entre outros.

Como Obter este Documento

Este documento pode ser obtido em http://cartilha.cert.br/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@cert.br.

Nota de *Copyright* e Distribuição

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.